Claims

What Is Claimed Is:

1. A method for providing information security comprising the steps of:

determining a digital signature verification error based on a received message header identifier associated with a public key certificate identifier; and

generating a digital signature verification map containing a plurality of acceptable message header identifiers associated with the public key certificate identifier.

2. The method of claim 1 wherein the step of generating the digital signature verification map includes storing at least one acceptable message header identifier as a digital signature verification map entry in response to determining the digital signature verification error.

3. The method of claim 1 wherein the step of generating the digital signature verification map includes mapping the plurality of acceptable message header identifiers on a per certificate subject identification data basis.

4. The method of claim 1 including the step of verifying a digital signature associated with received message information based on the digital signature verification map.

5. The method of claim 1 including the step of receiving digital signature verification map update data and updating the digital signature verification map with at least one acceptable message header identifier based on a received message header ID.

6. The method of claim 1 wherein the message header identifier includes at least one of data representing an email address of a sender, a telephone number of a sender and an identifier associated with a sending unit.

7. The method of claim 1 including the step of digitally signing the digital signature verification map to provide a trusted digital signature verification map.

8. The method of claim 1 including the steps of:

generating a trusted alias map containing the plurality of acceptable message identifiers and at least one associated subject alias; and

displaying the at least one subject alias in response to verifying a digital signature associated with the public key certificate identifier.

9. The method of claim 1 wherein the step of determining a digital signature verification error includes the steps of:

comparing the public key certificate identifier with the message header identifier to determine if a mismatch is detected;

if a mismatch is detected, generating a mismatch notification for an operator; and

verifying a digital signature based on a verification key associated with the public key certificate identifier.

10. A method for providing information security comprising the steps of:

determining a digital signature verification error based on a received message header identifier associated with a public key certificate identifier;

generating a digital signature verification map containing a plurality of acceptable message header identifiers associated with the public key certificate identifier by storing at least one acceptable message header identifier as a digital signature verification map entry in response to determining the digital signature verification error; and

verifying a digital signature associated with received message information based on the digital signature verification map.

11. The method of claim 10 wherein the step of determining a digital signature verification error includes the steps of:

comparing the public key certificate identifier with the message header identifier to determine if a mismatch is detected;

if a mismatch is detected, generating a mismatch notification for an operator; and

verifying a digital signature based on a verification key associated with the public key certificate identifier.

12. The method of claim 10 wherein the step of generating the digital signature verification map includes mapping the plurality of acceptable message header identifiers on a per certificate subject identification data basis.

13. The method of claim 11 including the step of receiving digital signature verification map update data and updating the digital signature verification map with at least one acceptable message header identifier based on a received message header ID.

14. The method of claim 10 wherein at least one of the plurality of message header identifiers includes at least one of data representing an email address of a sender, a telephone number of a sender and an identifier associated with a sending unit.

15. The method of claim 13 including the step of digitally signing the digital signature verification map to provide a trusted digital signature verification map.

16. The method of claim 10 including the steps of:

generating a trusted alias map containing the plurality of acceptable message identifiers and at least one associated subject alias; and

displaying the at least one subject alias in response to verifying a digital signature associated with the public key certificate identifier.

17. A method for providing information security comprising the steps of:

determining a digital signature verification error based on a received message header identifier associated with a public key certificate identifier; and

updating a digital signature verification map to add an acceptable message header identifier associated with the public key certificate identifier.

18. The method of claim 17 including the step of verifying a digital signature associated with received message information based on the digital signature verification map.

19. The method of claim 17 wherein the step of determining a digital signature verification error includes the steps of:

comparing the public key certificate identifier with the message header identifier to determine if a mismatch is detected;

if a mismatch is detected, generating a mismatch notification for an operator; and

verifying a digital signature based on a verification key associated with the public key certificate identifier.

20. An apparatus for providing information security comprising:

a processing module operative to determine a digital signature verification error based on a received message header identifier associated with a public key certificate identifier; and operative to generate a digital signature verification map containing a plurality of acceptable message header identifiers associated with the public key certificate identifier; and

memory, operatively coupled to the processing module, containing the digital signature verification map

21. The apparatus of claim 20 wherein the memory stores at least one acceptable message header identifier as a digital signature verification map entry.

22. The apparatus of claim 20 wherein the processing module maps the plurality of acceptable message header identifiers on a per certificate subject identification data basis.

23. The apparatus of claim 20 wherein the processing module includes a cryptographic engine operative to verify a digital signature associated with received message information based on the digital signature verification map.

24. The apparatus of claim 20 wherein the processing module updates the digital signature verification map with at least one acceptable message header identifier based on a received message header ID.

25. The apparatus of claim 20 wherein the message header identifier includes at least one of data representing an email address of a sender, a telephone number of a sender and an identifier associated with a sending unit.

26. The apparatus of claim 20 wherein the processing module digitally signs the digital signature verification map to provide a trusted digital signature verification map.

27. The apparatus of claim 20 wherein the processing module generates a trusted alias map containing the plurality of acceptable message identifiers and at least one associated subject alias, and displays the at least one subject alias in response verifying a digital signature associated with the public key certificate identifier.

28. The apparatus of claim 20 wherein the processing module determines a digital signature verification error by comparing the public key certificate identifier with the message header identifier to determine if a mismatch is detected; if a mismatch is detected, generating a mismatch notification for an operator; and verifying a digital signature based on a verification key associated with the public key certificate identifier.

29. A storage medium comprising:

memory containing executable instructions that when read by one or more processing units causes one or more processing units to:

determine a digital signature verification error based on a received message header identifier associated with a public key certificate identifier; and

generate a digital signature verification map containing a plurality of acceptable message header identifiers associated with the public key certificate identifier.

30. The storage medium of claim 29 wherein the memory contains executable instructions that cause the one or more processing units to generate the digital signature verification map by storing at least one acceptable message header identifier as a digital signature verification map entry in response to determining the digital signature verification error.

31. The storage medium of claim 29 wherein the memory contains executable instructions that cause the one or more processing units to map the plurality of acceptable message header identifiers on a per certificate subject identification data basis.

32. The storage medium of claim 29 wherein the memory contains executable instructions that cause the one or more processing units to verify a digital signature associated with received message information based on the digital signature verification map.

33. The storage medium of claim 29 wherein the memory contains executable instructions that cause the one or more processing units to receive digital signature verification map update data and update the digital signature verification map with at least one acceptable message header identifier based on a received message header ID.

34. The storage medium of claim 29 wherein the message header identifier includes at least one of data representing an email address of a sender, a telephone number of a sender and an identifier associated with a sending unit.

35. The storage medium of claim 29 wherein the memory contains executable instructions that cause the one or more processing units to digitally sign the digital signature verification map to provide a trusted digital signature verification map.

~~35~~ 36. The storage medium of claim 29 wherein the memory contains executable instructions that cause the one or more processing units to:

generate a trusted alias map containing the plurality of acceptable message identifiers and at least one associated subject alias; and

display the at least one subject alias in response verifying a digital signature associated with the public key certificate identifier.

~~36~~ 37. The storage medium of claim 29 wherein the memory contains executable instructions that cause the one or more processing units to determine a digital signature verification error by:

verifying a digital signature based on a verification key associated with the public key certificate identifier;

if verification is successful, comparing the public key certificate identifier with the message header identifier to determine if a mismatch is detected; and

if a mismatch is detected, generating a mismatch notification for an operator.

37. A method for providing information security comprising the steps of:

generating a trusted alias map containing the plurality of acceptable message identifiers and at least one associated subject alias; and

displaying the at least one subject alias in response to verifying a digital signature associated with a public key certificate identifier.

38. The method of claim 37 wherein the step of generating the trusted alias map includes digitally signing the trusted alias map, and wherein the method includes the step of verifying trusted alias map digital signature prior to displaying the at least one subject alias.